



**NCUA**  
National Credit Union Administration

# Privacy Impact Assessment for General Support System

---

Fiscal Year 2021

[This page intentionally left blank]





## About this Document

A Privacy Impact Assessment (PIA) is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements, to determine the privacy risks associated with an information system or activity, and to evaluate ways to mitigate privacy risks. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis.

Program offices and system owners are required to complete a PIA whenever they develop, procure, or use information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.<sup>1</sup> Completion of a PIA is a precondition for the issuance of an authorization to operate.<sup>2</sup>

## Basic Information about the System

**System Name:** NCUA General Support System (GSS)

**NCUA Office of Primary Interest (OPI):** Office of the Chief Information Officer

Threshold		
1	What is the status of the system/tool/application (for simplicity referred to as "system" going forward)?	Operational
2	Describe the system in 1-2 sentences.	The NCUA General Support System (GSS) provides the computing platform for all significant business applications for NCUA. The platform includes hardware, software, communications, network storage, databases, operating systems, and other infrastructure, security, and productivity applications.

<sup>1</sup> 44 U.S.C. § 3501, note; Pub. L. 107-347, § 208(b).

<sup>2</sup> OMB Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Act and Agency Privacy Management* (2013).



## Purpose and Authority

*The NCUA should only create, collect, use, process, store, maintain, disseminate, or disclose PII if it has authority to do so, and such authority should be identified in the appropriate notice.*

*The NCUA should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.*

Purpose and Authority		
1	What is the purpose of the system?	The NCUA General Support System (GSS) provides the computing platform for all significant business applications of NCUA. The platform includes all major IT hardware, software, communications, network storage, central databases, operating systems, and other minor, infrastructure, security-related, and productivity applications.
2	How is the PII collected/maintained/used in the system relevant and necessary to achieve the purpose described above?	NCUA OPI's use OPI-owned applications that reside on the GSS computing platform to collect, create, maintain, and/or distribute the PII of NCUA employees, state examiners, credit unions, and contractors.
3	What is the legal authority to collect, maintain, use, or share the PII contained in the system?	The legal authorities to collect, maintain, use, or share PII on the NCUA GSS include Title 5, United States Code, Section 301 and Title 12, United States Code, Chapter 14 (The Federal Credit Union Act). The authorities that permit specific systems on the GSS to collect, use, maintain, and share PII are addressed in specific Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs).



## Minimization

*The NCUA should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish that purpose.*

The NCUA recognizes the increased sensitivity of Social Security numbers (SSNs) and therefore makes every effort to limit the collection and maintenance of them. The NCUA also limits its collection of other types of PII to those that are necessary.

SSNs		
<b>1</b>	<i>Will the system collect, maintain, or share social security numbers?</i>	<ul style="list-style-type: none"><li>• Yes</li></ul>
<b>1.1</b>	<i>Of who?</i>	<ul style="list-style-type: none"><li>• CU Members</li><li>• CU Officers, Employees, Volunteers</li><li>• NCUA Employees/Contractors</li><li>• Others: SSAs</li></ul>
<b>1.2</b>	<i>What is the law that authorizes this collection of SSNs?</i>	<ul style="list-style-type: none"><li>• The legal authorities to operate the NCUA GSS are Title 5, United States Code, Section 301 and Title 12, United States Code, Chapter 14 (The Federal Credit Union Act). The authorities that permit specific systems on the GSS to collect, use, maintain, and share PII are addressed in specific PIAs and SORNs.</li></ul>
<b>1.3</b>	<i>Will the system collect, maintain, or share social security numbers?</i>	<ul style="list-style-type: none"><li>• NCUA OPIs use OPI-owned applications that reside on the GSS computing platform to collect, create, maintain, and/or distribute the PII of NCUA employees, state examiners, credit unions, and contractors. The platform includes all major IT hardware, software, communications, network storage, central databases, operating systems, and other minor, infrastructure, security-related, and productivity applications. The NCUA GSS relies on the OPI application data owners to complete PIAs to document</li></ul>



		the information collection reason, as required.
<b>1.4</b>	<i>Why would using a less sensitive identifier or group of identifiers be insufficient</i>	<ul style="list-style-type: none"> <li>NCUA OPIs use OPI-owned applications that reside on the NCUA GSS. The NCUA OPI application PIAs describe the intended agency use for PII that is collected, created, maintained, and/or distributed.</li> </ul>
<b>1.5</b>	<i>Approximately how many unique SSNs will be maintained in the system?</i>	<ul style="list-style-type: none"> <li>More than 10,000</li> </ul>

PII		
<b>1</b>	<i>Basic Demographic</i>	<ul style="list-style-type: none"> <li>Birthdate, Age</li> <li>Drivers License Number or State ID Number</li> <li>Email Address</li> <li>First Name</li> <li>Home Address</li> <li>Last Name</li> <li>Middle Name (or initial)</li> <li>Phone Number</li> <li>Race or Ethnicity</li> <li>Sex/Gender</li> </ul>
<b>1.1</b>	<i>Who is it collected for?</i>	<ul style="list-style-type: none"> <li>CU Members</li> <li>CU Officers, Employees, Volunteers</li> <li>NCUA Employees/Contractors</li> </ul>
<b>2</b>	<i>Medical and Family</i>	<ul style="list-style-type: none"> <li>Emergency Contact</li> <li>Information about Spouse(s), Children, or other Family Members</li> <li>Marital Status or Marriage/Divorce Records</li> <li>Medical History</li> <li>Reasonable Accommodation Information</li> </ul>
<b>2.1</b>	<i>Who is it collected for?</i>	<ul style="list-style-type: none"> <li>NCUA Employees/Contractors</li> </ul>
<b>3</b>	<i>Financial</i>	<ul style="list-style-type: none"> <li>Account Number</li> </ul>
<b>3.1</b>	<i>Who is this information collected for?</i>	<ul style="list-style-type: none"> <li>NCUA Employees/Contractors</li> </ul>
<b>4</b>	<i>Biometric</i>	<ul style="list-style-type: none"> <li>Photograph</li> <li>Signature</li> <li>Voice Recording</li> </ul>



<b>4.1</b>	<i>Who is this information collected for?</i>	<ul style="list-style-type: none"><li>• NCUA Employees/Contractors</li></ul>
<b>5</b>	<i>Employment and Education</i>	<ul style="list-style-type: none"><li>• Employment History</li></ul>
<b>5.1</b>	<i>Who is this information collected for?</i>	<ul style="list-style-type: none"><li>• NCUA Employees/Contractors</li></ul>
<b>6</b>	<i>Information Technology (IT)</i>	<ul style="list-style-type: none"><li>• Answers to Security Questions</li><li>• Digital Certificate</li><li>• Login/Activity Records</li><li>• Password</li><li>• Tracking Data (Cookies, Beacons, etc.)</li><li>• Unique Device Identifier</li><li>• Username</li></ul>
<b>6.1</b>	<i>Who is this information collected for?</i>	<ul style="list-style-type: none"><li>• NCUA Employees/Contractors</li></ul>
<b>7</b>	<i>NCUA Employment</i>	<ul style="list-style-type: none"><li>• Drug Test Results</li><li>• NCUA Email Address</li><li>• NCUA Employee ID Number</li><li>• NCUA Employment Performance Appraisal Information</li><li>• NCUA iPhone Number</li><li>• NCUA issued Credit Card Number and associated information</li><li>• NCUA Office Phone Number</li><li>• NCUA Training History</li></ul>
<b>7.1</b>	<i>Who is this information collected for?</i>	<ul style="list-style-type: none"><li>• NCUA Employees/Contractors</li></ul>

## Collection and Consent

*The NCUA should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.*

*The NCUA should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. The NCUA should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.*

The NCUA endeavors both to collect information from the subject individual, and to attain affirmative informed consent, whenever possible. The NCUA's use of Privacy



Act statements and privacy notices on forms are critical to this effort. For more information see the Transparency section below.

Collection and Consent		
1	<i>What are the sources from which the PII will be collected?</i>	<ul style="list-style-type: none"><li>• Other: Decisions regarding collection, including PII, are made by the respective owners of the individual applications residing on the NCUA GSS. More information regarding implementation of this control at the application level is reflected in the PIA for each.</li></ul>
2	<i>How will the information be collected?</i>	<ul style="list-style-type: none"><li>• From another Information System</li><li>• Web-based Form or Email</li><li>• Other: The NCUA GSS is reliant on the PIAs for the OPI business applications to describe the notice, the opportunity to approve or decline, and the consent of individuals for their respective collections of PII.</li></ul>
3	<i>Will the individuals whose information is collected/maintained in the system consent to their personal information?</i>	<ul style="list-style-type: none"><li>• Not specifically, but the individuals consented to providing the information originally and likely anticipated that their information would also be maintained and used this way.</li></ul>
4	<i>Will individuals be able to “opt-out” by declining to provide PII or by consenting only to a particular use?</i>	<ul style="list-style-type: none"><li>• No</li></ul>

## Procedures to Address Individuals’ Privacy Related Complaints and Inquiries

The Privacy team knows that complaints, concerns, and questions from individuals can be a valuable source of input that improves operational models, uses of technology, data collection practices, and privacy safeguards. To facilitate this type of feedback, the Privacy team has established the Privacy Complaint Process to receive and respond to complaints, concerns, and questions from individuals about the NCUA’s privacy practices. The process is described on the [NCUA’s privacy website](#). The Privacy team appropriately records and tracks complaints, concerns, and questions to ensure prompt remediation.





## Maintenance and Use

*The NCUA should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.*

The NCUA implements, documents, and tests security and privacy controls as required by applicable NIST and OMB guidance. Access controls are of particular importance with regard to protecting individuals' privacy. Records management, both keeping records for the required time frame and timely destroying or accessions them, is also a key component of managing privacy risks.

Maintenance and Use		
1	Which statement is most accurate?	<ul style="list-style-type: none"><li>• NCUA owns the System</li></ul>
2	Who has access to PII in the system?	<ul style="list-style-type: none"><li>• NCUA Employees</li><li>• NCUA Contractors</li></ul>
3	Which roles have access to PII in the system?	<ul style="list-style-type: none"><li>• Some System Users</li><li>• System Administrators</li><li>• Developers</li></ul>

Records Management		
1	Which records retention schedule(s) will apply to this system?	<ul style="list-style-type: none"><li>• General Record Schedule - Technology (GRS 3.0)</li></ul>



## Transparency

---

*The NCUA should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.*

The NCUA’s transparency efforts include providing adequate notice to individuals prior to collection of their PII. The NCUA achieves this with Privacy Act statements, or privacy notices (the latter if the collection is not associated with a Privacy Act System of Records), and compliance with the Paperwork Reduction Act.<sup>3</sup> The NCUA also publishes Systems of Records Notices in the Federal Register and makes them available on [the privacy page of the NCUA’s website](#).

Transparency		
1	Will any forms or surveys be used to collect the information?	<ul style="list-style-type: none"><li>No</li></ul>

SORNs		
1	Is the information in the system retrieved by a personal identifier?	<ul style="list-style-type: none"><li>Yes</li></ul>
2	Applicable SORN	<ul style="list-style-type: none"><li>-</li></ul>

---

<sup>3</sup> See the Collection and Consent section above.



## Accountability

---

*The NCUA should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. The NCUA should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.*

### Compliance with the Fair Information Privacy Principles

As evidenced by this PIA (and the other information publicly available on [the privacy page of NCUA's website](#)), the NCUA is committed to achieving and maintaining compliance with the Fair Information Privacy Principles.

### Roles and Responsibilities of NCUA Staff

As detailed in the NCUA Acceptable Use Policy and applicable Rules of Behavior, all NCUA staff are responsible for protecting PII from unauthorized exposure and for reducing the volume and types of PII necessary for program functions. Staff must protect all PII that they handle, process, compile, maintain, store, transmit, or report on in their daily work.

To protect PII, staff must use proper collection, storage, transportation, transmission, and disposal methods, must not access PII beyond what they need to complete their job duties, and must not disclose PII to unauthorized parties. Managers are also responsible for providing their subordinates with context-specific practical guidance about protecting PII.

All NCUA staff are required to review and acknowledge receipt and acceptance of applicable Rules of Behavior upon gaining access to the NCUA's information systems and associated data.

Failure to protect PII may result in administrative sanctions, and criminal and/or civil penalties.<sup>4</sup>

---

<sup>4</sup> 5 U.S.C. § 552a(i)(3); NCUA Computer Security Rules of Behavior.



## Training

Together with the Office of Human Resources, the Privacy team ensures that new employees complete mandatory privacy training, and all existing employees and contractor employees complete privacy refresher training once every fiscal year. NCUA staff electronically certify acceptance of their privacy responsibilities as a part of annual privacy refresher training. The Privacy team keeps auditable records of completion of all mandatory trainings.

## Analysis and Approval

---

This PIA was approved by or on behalf of the Senior Agency Official for Privacy. Below are additional details regarding the review and approval of the PIA.

Analysis and Approval	
<b>Privacy Risk:</b>	Acceptable
<b>Approval Date:</b>	December 21, 2020